UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/589,476	06/20/2007	Stefan Kistner	23697	8372

535 7590 10/26/2010

KF ROSS PC
5683 RIVERDALE AVENUE
SUITE 203 BOX 900
BRONX, NY 10471-0900

EXAMINER	
LEE, JASON T	

ART UNIT	PAPER NUMBER
2438	

NOTIFICATION DATE	DELIVERY MODE
10/26/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

EMAIL@KFRPC.COM
ereyes@kfrpc.com

Office Action Summary	Application No.	Applicant(s)	
	10/589,476	KISTNER, STEFAN	
	Examiner	Art Unit	
	JASON LEE	2438	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 June 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *14 August 2006* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. The following is a non-final office action in response to applicant's preliminary amendment filed on June 20, 2007. The original application was filed on August 14, 2006. Claims 1-20 have been amended. No claims have been added. No claims have been cancelled. Therefore, claim 1-20 are pending and addressed below.

Drawings

2. The drawings are objected to because the drawings fail to show the details and not in a sufficient quality with the feature of the invention. For example, in the FIG 6 of the drawing with flowchart, there is no corresponding steps with the explanation of the chart can be found. Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the

examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

3. For the record, Applicant's amendment of Specification filed on June 20, 2007 has been accepted.

4. On Specification page 2 line 3, recites "In particular the USB port present in modern computer systems is a danger, since so-called memory sticks that can be connected to USB ports only have a small size und are therefore not noticed easily", where und appears a typographic error. Appropriate correction is required.

Priority

5. This application is related to and claimed the benefits of Germany Patent application No.10 2004 009 065.3 filed 02/23/2004.

Examiner's Note

6. Claims 1-20 are considered to be in compliance with 35 U.S.C. 101 as the claimed methods cannot be performed without use of a hardware computing system.

Claim Rejections - 35 USC § 112

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. Claims 1, 2, 4, 5, 7, 9, 11, 13, 14 and 17 are rejected under 35 U.S.C 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

For example, claim 1 recites the limitation "in particular with use of exchangeable and/or removable data carriers and/or storage medium, where in particular peripherals are connectable to the computer system, characterized by the following steps: analysis of the protocol and of the data stream from and to data carriers and/or storage media and/or peripheral devices;". It is not clear the "removable" data carriers and/or storage medium and "data carrier and/or storage media" are the same. Claim 1 recites" data system" where is no clear definition on the instant specification teaches the "data system". There is insufficient antecedent basis for this limitation in the claim. (e.g. the data stream).

Claim 2 recites "determining that an encryption of all blocks of the data carrier/storage medium or an encryption of all files before storage on the data carrier/storage medium and that an encryption of several files before storage on the data carrier/storage medium is carried out." It is not clear the "storage" means.

Claim 4 recites "the cryptographic encryption is temporarily suspended when particular features are shown". It is not clear what "particular features" are.

Claim 5 recites "when a data carrier or a storage medium without data system is used, an encryption of all blocks is carried out and access is prevented." The claim limitation is unclear for "when a data carrier or a storage medium without data system is used".

Claim 7 recites "network based data carriers or network based storage media are used." There is no description in the instant Specification for "network based data carriers or network based storage media.

Claim 9 recites "...and taking the analysis into account for establishing the classification on the basis of the physical connection or the properties of the devices." There is insufficient antecedent basis for this limitation in the claim. What is "the devices"?

Claim 11 recites "wherein the encryption is performed in accordance with a first cryptographic method, and thereafter is again encrypted by means of a second cryptographic method." There is no description in the instant Specification for "first cryptographic method and "second cryptographic method".

Claim 13 recites "step of preventing encryption of the data". There is no teaching about what is "preventing encryption of the data". There is description in Specification how the preventing encryption of the data is done.

Claim 14 recites "of preventing the encryption only at predetermined times." There is no teaching about what means by "only at predetermined times".

Claim 17 recites "method according to claim 1 wherein actions that are performed by means of the computer system are recorded." There is insufficient antecedent basis for this limitation in the claim. No "actions" recited in the claim 1.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 1-13, 15, 16 and 18-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wilson (US 2002/0166053 A1), hereinafter Wilson, in view of Gupta

(US 2004/0073947 A1) hereinafter Gupta, further in view of Tatebayashi et al (US 6,182,215 B1) hereinafter Tatebayashi.

As for claim 1:

Wilson discloses **a method of preventing the loss of confidentiality of electronically stored data in a computer system,** (see Wilson [0049] "prevents unauthorized users from accessing the data in storage") **which data in particular is organized as a data system and or subdivided into blocks,** (see Wilson [0036] "a technique for encrypting data in the files 12 and swap file 28 to prevent unauthorized access to such files. In certain implementations, the encryption programs are implemented in the paging system 22 and file system 24 to ensure encryption of any data written to storage 8, whether the paging system 22 is writing data to the swap file 18 or the file system 24 is writing data to files 12. ") **in particular with use of exchangeable and/or removable data carriers and/or storage medium, where in particular peripherals are connectable to the computer system,** (see Wilson [0023] "The computer 2 is further capable of accessing data in a removable storage medium 32, such as a removable magnetic disk (e.g., floppy disk, ZIP disk, JAZ disk**), removable optical disk (e.g., CD-ROM, DVD, etc.), a Personal Computer Memory Card International Association (PCMCIA) card, removable flash card, etc.") **characterized by the following steps: analysis of the protocol and of the data stream from and to data carriers and/or storage media and/or peripheral devices;** (see Wilson [0037] "data structures the paging system 22 and file system 24 maintain in the kernel 20 to provide for encryption of the files 12 and swap files 18. To enable users who have properly logged onto the

system to access files 12 associated with groups of which they are a member, the file system 24 maintains a private key index 90 in the kernel 20 of system memory 6 for the private keys users with active sessions have provided to decrypt files") **establishment of a classification, in particular for differentiation between nonremovable and removable data carriers and/or storage media; determination on the basis of the established classification, whether an encryption of the electronically stored data is required for preventing the loss of confidentiality of the data and, depending on this determination, possibly adding a cryptographic encryption to the data system on a removable data carrier and/or a removable storage medium, or performing a cryptographic encryption on all or several blocks of the removable data carrier and/or of the removable storage medium.** (see Wilson [0009] " for encrypting data in a computer in communication with a volatile memory and non-volatile storage device. Pages in the volatile memory to move to a swap file in the non-volatile storage device as part of a virtual addressing system are encrypted. The encrypted pages are then moved from the volatile memory to the swap file. The pages in the swap file are decrypted when moving the pages back into memory. The decrypted pages are then moved back into memory.")

Wilson discloses a method for preventing unauthorized access for the data file system in a computer system includes a removable storage medium with a cryptographic encryption to the data system (e.g. swap files). Wilson does not explicitly disclose **"establishment of a classification, in particular for differentiation between nonremovable and removable data carriers and/or storage media;"** however, Gupta

discloses as claimed. (see Gupta [0088] "Computer 342 further includes a hard disk drive 356 for reading from and writing to a hard disk, not shown, connected to bus 348 via a hard disk drive interface 357 (e.g., a SCSI, ATA, or other type of interface); a magnetic disk drive 358 for reading from and writing to a removable magnetic disk 360, connected to bus 348 via a magnetic disk drive interface 361; and an optical disk drive 362 for reading from and/or writing to a removable optical disk 364 such as a CD ROM, DVD, or other optical media, connected to bus 348 via an optical drive interface 365. The drives and their associated computer-readable media provide nonvolatile storage of computer readable instructions, data structures, program modules and other data for computer 342" and [0032] "storage device 168 may include fixed storage media (e.g., a typical magnetic hard disk drive) and/or removable storage media (e.g., a DVD). ") Gupta discloses the storage device includes fixed storage media and/or removable storage media as claimed. Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teaching of Wilson within the combination system of Gupta because they are analogous in the secure network using encryption for the data file system to protect the data contents. One of the ordinary skills in the art would have been motivated to incorporate the teaching to improve the system operation efficiently.

The combination of Wilson and Gupta does not discloses **"determination on the basis of the established classification, whether an encryption of the electronically stored data is required for preventing the loss of confidentiality of the data and, depending on this determination"** However, Tatebayashi discloses as claimed. (see

Tatebayashi column 5 lines 36-52 " a type information storage unit for storing the type information showing the device type of the present information device out of the n different device types; and a determination unit for determining, on being informed of the type information of the other information device with which the communication is to be performed, an encryption utilization protocol shown by protocol correspondence information that is associated in the table stored in the table storage unit to the combination of the type information of the other information device and the type information of the present information device as the encryption utilization protocol which is to be used in the communication, and wherein the communication unit has a protocol correspondence communication unit that corresponds to the encryption utilization protocol determined by the determination unit perform the communication using the determined encryption utilization protocol.")

Tatebayashi discloses a determination unit for storage unit in computer system for determining using the encryption protocol to protect the data in the storage unit.

It would has been obvious to one having the ordinary skill in the art at the time the invention was made to modify the modified-invention of Wilson to include the determination on the base of the storage medium in the data system for preventing the access of data access in the system because they are in the same field of endeavor of protecting data access and one of ordinary skill in the art would have been motivated to incorporate the teaching so to prevent unauthorized acts such as copyright protection. (see Tatebayashi column 6 lines 12-20)

As for claim 2:

The combination of Wilson, Gupta and Tatebayashi discloses **the method according to claim 1** above, **further comprising the step of determining that an encryption of all blocks of the data carrier/storage medium or an encryption of all files before storage on the data carrier/storage medium and that an encryption of several files before storage on the data carrier/storage medium is carried out.** (see Wilson [0012] "A determination is made of the group associated with the target file and the first encryption code for the group. The determined first encryption code is used to encrypt the target file if the I/O request is a write operation to write the target file to the non-volatile storage device.")

As for claim 3:

The combination of Wilson, Gupta and Tatebayashi discloses **the method according to claim 1** above, **wherein a cryptographic encryption is added to each data system on nonremovable or nonexchangeable data carriers or storage media.** (see Wilson [0010] "codes are generated to use to encrypt and decrypt the pages. The codes may comprise a public/private key pair generated using a public key cryptography algorithm. One key of the pair is used to encrypt the pages moved to the swap file and the other key of the pair is used to decrypt the page when moving the page from the swap file to the volatile memory." And [0012] "a method for encrypting files in a computer file system in communication with a volatile memory and a non-volatile storage device.")

As for claim 4:

The combination of Wilson, Gupta and Tatebayashi discloses **the method according to claim 3** above, **wherein the cryptographic encryption is temporarily suspended when particular features are shown.** (see Wilson [0042] "system configuration files should never be encrypted because they must be accessed in order to perform basic operations. If such configuration files are encrypted, then the operating system would not be able to initialize. To leave configuration files unencrypted, the permissions 56 in the file metadata 50 (FI;G. 2) for the configuration files would be set to globally accessible. Similarly, an owner of a file may set a data file's permissions 56 to globally accessible to leave such files unencrypted for anyone to access and read.") Wilson discloses there are particular features (e.g. system configuration files or owner of the files) can have the files unencrypted. (temporarily suspended for encryption).

As for claim 5:

The combination of Wilson, Gupta and Tatebayashi discloses **the method according to claim 1** above, **wherein when a data carrier or a storage medium without data system is used, an encryption of all blocks is carried out and access is prevented.** (see Wilson [0036] "implementations provide a technique for encrypting data in the files 12 and swap file 28 to prevent unauthorized access to such files. In certain implementations, the encryption programs are implemented in the paging system 22 and file system 24 to ensure encryption of any data written to storage 8, whether the paging system 22 is writing data to the swap file 18 or the file system 24 is writing data to files 12." And [0037] "data structures the paging system 22 and file system 24 maintain in the kernel 20 to provide for encryption of the files 12 and swap

files 18. To enable users who have properly logged onto the system to access files 12 associated with groups of which they are a member, the file system 24 maintains a private key index 90 in the kernel 20 of system memory 6 for the private keys users with active sessions have provided to decrypt files 12.") Wilson discloses the encryption for the page system to prevent the unauthorized access to such files.

As for claim 6:

The combination of Wilson, Gupta and Tatebayashi discloses **the method according to claim 1** above, **wherein an encryption is performed when removable data carriers and or removable storage media are used.** (see Tatebayashi column 4 line 49 to column 5 line 2 " at least one encryption utilization protocol that can be executed by the present information device out of the plurality of encryption utilization protocols, to another information device in the communication system with which communication is to be performed....from a combination of the type information of the present information device and type information received from the other information device with which the communication is to be performed")

It would has been obvious to one having the ordinary skill in the art at the time the invention was made to modify the modified-invention of Wilson to include the encryption on the device (e.g. removable data carriers or storage media) and one of ordinary skill in the art would have been motivated to incorporate the teaching so to prevent unauthorized acts or infringements.

As for claim 7:

The combination of Wilson, Gupta and Tatebayashi discloses **the method according to claim 1** above, **wherein an encryption is performed when removable data carriers or nonremovable storage media, or network based data carriers or network based storage media are used.** (see Wilson [0021] "The computer 2 is capable of accessing a storage system 8, which may comprise one or more hard disk drives or any other non-volatile storage devices known in the art. The storage 8 includes an operating system 10, files 12, user information 14 providing individual user login information, group information 16 providing information for groups of users, and a swap file 18 used during virtual memory operations. The storage 8 may comprise a local storage space and/or a network storage space.")

As for claim 8:

The combination of Wilson, Gupta and Tatebayashi discloses **the method according to claim 1** above, **wherein when a data carrier or a storage medium is connected to a multifunctional interface or a multifunctional bus, the functionality of the interfaces or the buses is maintained and an encryption is only performed on data streams that are further transmitted to the interface or the bus for storing the data.** (see Wilson [0042] "In certain implementations, certain type of files may be left unencrypted at all times. For instance, system configuration files should never be encrypted because they must be accessed in order to perform basic operations. If such configuration files are encrypted, then the operating system would not be able to initialize." And Gupta [0089]" A number of program modules may be stored on the hard disk, magnetic disk 360, optical disk 364, ROM 350, or RAM 352, including an operating

system 370, one or more application programs 372, other program modules 374, and program data 376. A user may enter commands and information into computer 342 through input devices such as keyboard 378 and pointing device 380. Other input devices may include a microphone, joystick, game pad, satellite dish, scanner, or the like. These and other input devices are connected to the processing unit 344 through an interface 368 that is coupled to the system bus (e.g., a serial port interface, a parallel port interface, a universal serial bus (USB) interface, etc.)") The combination of Wilson and Gupta discloses that the data streams has connection interface (e.g. USB), an encryption is performed, but certain type of files may be left unencrypted at all times (e.g. Operation system files which is not stored in the data carrier that is connected to a multifunctional interface (e.g. USB port).

As for claim 9:

The combination of Wilson, Gupta and Tatebayashi discloses **the method according to claim 1** above, **further comprising the steps of performing an analysis of the interface or the bus to which a data stream shall be transmitted and taking the analysis into account for establishing the classification on the basis of the physical connection or the properties of the devices.** (see Gupta [0088]-[0089]" "Computer 342 further includes a hard disk drive 356 for reading from and writing to a hard disk, not shown, connected to bus 348 via a hard disk drive interface 357 (e.g., a SCSI, ATA, or other type of interface); a magnetic disk drive 358 for reading from and writing to a removable magnetic disk 360, connected to bus 348 via a magnetic disk drive interface 361; and an optical disk drive 362 for reading from and/or writing to a

removable optical disk 364 such as a CD ROM, DVD, or other optical media, connected to bus 348 via an optical drive interface 365. The drives and their associated computer-readable media provide nonvolatile storage of computer readable instructions, data structures, program modules and other data for computer 342" and [0032] "storage device 168 may include fixed storage media (e.g., a typical magnetic hard disk drive) and/or removable storage media (e.g., a DVD). "interface 368 that is coupled to the system bus (e.g., a serial port interface, a parallel port interface, a universal serial bus (USB) interface")

Examiner supplies the same rational for the combination of the reference as in claim 1 above.

As for claim 10:

The combination of Wilson, Gupta and Tatebayashi discloses **the method according to claim 1** above, **wherein cryptographic methods for encryption are applied.** (see Wilson [0010] "codes are generated to use to encrypt and decrypt the pages. The codes may comprise a public/private key pair generated using a public key cryptography algorithm. One key of the pair is used to encrypt the pages moved to the swap file and the other key of the pair is used to decrypt the page when moving the page from the swap file to the volatile memory." And [0012] "a method for encrypting files in a computer file system in communication with a volatile memory and a non-volatile storage device." And [0013] "An encryption code is generated to encrypt a file and a decryption code is generated to decrypt one file encrypted with the encryption code.")

As for claim 11:

The combination of Wilson, Gupta and Tatebayashi discloses **the method according to claim 1** above, **wherein the encryption is performed in accordance with a first cryptographic method, and thereafter is again encrypted by means of a second cryptographic method.** (see Wilson [0012] "The files in the file system are associated with groups. For each group, provided is a group identifier, a list of user identifiers of users allowed to access files in the group, and a first encryption code. A second encryption code is received for one user identifier. An input/output (I/O) request from a requesting user identifier with respect to a target file is received, wherein one second encryption code has been received for the user identifier.")

As for claim 12:

The combination of Wilson, Gupta and Tatebayashi discloses **the method according to claim 1** above, **further comprising the step of, during a reading process from a data carrier or storage medium that is at least partially encrypted, performing a decryption of the data.** (see Wilson [0012] "If the requesting user identifier is in the list, then the second encryption code for the user identifier is used to decrypt the target file if the I/O request is a read operation to read the target file from the non-volatile storage device.")

As for claim 13:

The combination of Wilson, Gupta and Tatebayashi discloses **the method according to claim 1** above, **further comprising the step of preventing encryption of the data by using hardware with an integrated key or by using a password or by recognizing and controlling biometric data of a user.** (see Wilson [0026] "Login ID

72: this is the name provided in addition to the password, also known as the user name.")

As for claim 15:

The combination of Wilson, Gupta and Tatebayashi discloses **the method according to claim 1** above, **wherein for the encryption, keys are used that are formed by combination of different parts, whereby in particular several computer systems can be combined in groups, the keys of a group of computer systems having a common part as well as a respective individual part.** (see Wilson [0010] ""codes are generated to use to encrypt and decrypt the pages. The codes may comprise a public/private key pair generated using a public key cryptography algorithm. " and [0012] "The files in the file system are associated with groups. For each group, provided is a group identifier, a list of user identifiers of users allowed to access files in the group, and a first encryption code. A second encryption code is received for one user identifier. An input/output (I/O) request from a requesting user identifier with respect to a target file is received, wherein one second encryption code has been received for the user identifier.")

As for claim 16:

The combination of Wilson, Gupta and Tatebayashi discloses **the method according to claim 15** above, **wherein the key that is to be applied for the encryption and decryption can be determined or stored in a data base for being requested or is integrated in a hardware or is determined from biometric data of a user by using an algorithm.** (see Wilson [0010] "codes are generated to use to encrypt and decrypt

the pages. The codes may comprise a public/private key pair generated using a public key cryptography algorithm.")

As for claim 18:

The combination of Wilson, Gupta and Tatebayashi discloses **the method according to claim 1** above, **wherein the computer system has an operating system that at least distinguishes between a kernel mode and a user mode, the method being at least partially implemented in the kernel mode.** (see Wilson [0022] "After initialization, the operating system 10 loads essential services and programs required by other parts of the operating system and applications into an area of the system memory 6 referred to as a kernel 20. The operating system 10 may comprise any operating system program known in the art, e.g., Solaris, Windows, etc. Typically, the kernel 20 is responsible for memory management, process and task management, and disk management. The kernel 20 further includes a paging system 22 and a file system 24. The paging system 22 implements a virtual memory system that is capable of swapping data between the memory 6 to the swap file 18 in local storage 8 in a manner known in the art to increase the available space of the system memory 6. The file system 24 comprises the operating system component that organizes and provides access to files in a manner known in the art, such as providing a hierarchical file system using directories to organize files into a tree structure. The system memory 6 farther includes additional operating system and application programs and data 26.") Wilson teaches the kernel and user mode (application program) of the operation system and kernel mode is implemented.

As for claim 19:

The combination of Wilson, Gupta and Tatebayashi discloses **the method according to claim 1** above, **wherein a logic combination of several computer systems within a group is performed, wherein within the group the cryptographic encryption is mutually suspended, wherein the cryptographic encryption is maintained with respect to external sources.** (see Wilson [0041] "FIG. 8 illustrates logic implemented in the file system 24 to authenticate a user that begins a session and load the encryption keys needed to provide that user access to files in the group to which the user belongs, such as any entries 92 and 102 in the private key 30 and public key 100 indexes. Control begins at block 150 with the file system 24 receiving a login ID and password for a login attempt. The file system 24 scans (at block 152) the user information 14 to determine (at block 154) whether the user information 14 includes an entry 70 having the received login ID and password values in the corresponding entries 72 and 74")

As for claim 20:

The combination of Wilson, Gupta and Tatebayashi discloses **the method according to claim 1** above, **wherein during access on a data carrier or storage medium, it is determined whether an encryption of all blocks of the data carrier/storage medium or an encryption of all files on the data carrier/storage medium or an encryption of several files is present, and that an encryption of the requested data is performed.** (see Wilson [0047]-[0049] "The result of the logic of FIG. 9 is that for those group IDs using encryption, the file system 24 writes all files for that group ID

encrypted to storage 8... if the user ID is a member of the group, i.e., on the list 88, and read access is granted in the permissions 56 (FIG. 2), then a determination is made (at block 258) whether a public key is used with the group ID, i.e., the group is encrypted. If not, read access is granted (at block 260) to the requesting user ID as the requesting user ID is allowed access and no decryption is necessary as the file is not encrypted, i.e., not associated public key 86 in the group information entry 80 (FIG. 4). ....if (at block 262) there is a matching entry 92 in the private key index 90, then the file system 24 determines (at block 264) whether the requested file is in memory 6, i.e., a cache hit.")

Wilson teaches whether an encryption is performed of all the files or partial files that matches the request files to be performed with encryption.

10. Claims 14 and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wilson, Gupta and Tatebayashi as above; further in view of Kohara et al (US 2003/0182566 A1), hereinafter Kohara.

As for claim 14:

The combination of Wilson, Gupta and Tatebayashi discloses **the method according to claim 13** above, none of them discloses **further comprising the step of preventing the encryption only at predetermined times.** However, Kohara teaches the encryption only at predetermined times. (see Kohara [0065] "encryption storage apparatus 11 can be arranged so that after a lapse of a predetermined time period from the allocation of the encryption key c to the user, the encryption key c corresponding to the key number a2 is not provided to the encryption section 5 and the decryption section

6 even if the key number a2 is inputted. This makes the encryption key c unusable after a lapse of a predetermined time period from allocation, so that it is possible to prevent the same encryption key c from being possessed by the user for a long time.")
It would has been obvious to one having the ordinary skill in the art at the time the invention was made to modify the modified-invention of Wilson to include the predetermined times as taught by Kohara because they are in the same field of endeavor of protecting data access and one of ordinary skill in the art would have been motivated to incorporate the teaching so to prevent the invalidation of the encryption key to further protect the data system confidentiality.

As for claim 17:

The combination of Wilson, Gupta and Tatebayashi discloses **the method according to claim 1** above, none of them discloses **wherein actions that are performed by means of the computer system are recorded.** However, Kohara teaches the recording. (see Kohara [0066] "records the date and time when the key number a2 is assigned (when the encryption key c is allocated), and the key management section 7 invalidate the encryption key c corresponding to the relevant allocation frame after a lapse of a predetermined time period from the date and time of recording.")
It would has been obvious to one having the ordinary skill in the art at the time the invention was made to modify the modified-invention of Wilson to include the recording as taught by Kohara because they are in the same field of endeavor of protecting data access and one of ordinary skill in the art would have been motivated to incorporate the

teaching so to prevent the invalidation of the encryption key to further protect the data system confidentiality.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JASON LEE whose telephone number is (571)270-7477. The examiner can normally be reached on Monday-Friday 9/5/4 (altering Friday off).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Taghi T Arani can be reached on (571)272-3787. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/J. L./
Examiner, Art Unit 2438

/Taghi T. Arani/

Supervisory Patent Examiner, Art Unit 2438